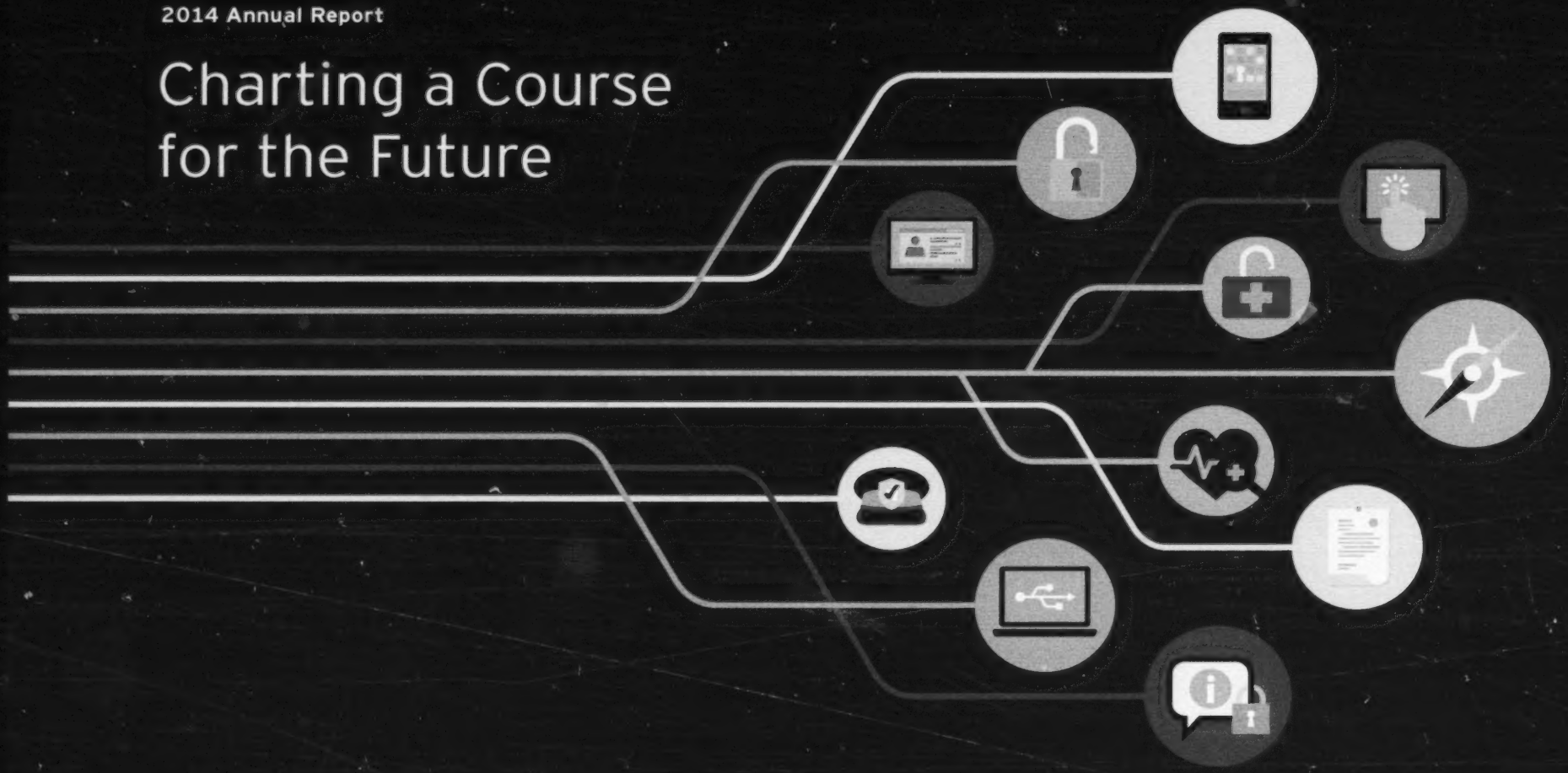
2014 Annual Report

Charting a Course for the Future



Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

@IPCInfoPrivacy

Letter to the Speaker

May 26, 2015

The Honourable Dave Levac
Speaker of the Legislative Assembly of Ontario

Dear Speaker,

I have the honour to present the 2014 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1 to December 31, 2014.

Please note that additional reporting from 2014, including the full array of statistics, analysis and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca.

Sincerely yours,

Brian Beamish
Commissioner

Table of Contents

Commissioner's Message 1

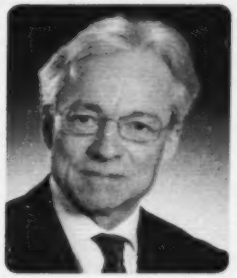
Access
Access to Information 3
Open Government 3
Significant Access Decisions 4
Judicial Reviews 5
Recommendation 6

Privacy
Protection of Privacy 7
Situation Tables 7
Police Body-Worn Cameras 7
Crossing the Line 8
Police Record Checks 9
Recommendation 10

Health Privacy
PHIPA 10th Anniversary 11
Unauthorized Access 11
ConnectingPrivacy 13
Recommendation 13

Statistics
Overall Requests 14
Overall Appeals 14
2014 At A Glance 14
FOI Requests and Appeals 17
Health Privacy 18
Privacy Complaints 19
Judicial Reviews 19

Financials 20



Charting a Course for the Future

It is said that with every change comes opportunity. With that in mind, I am looking forward to what lies ahead as I begin my term as Information and Privacy Commissioner. It was over a quarter-century ago that Justice Sidney Linden opened our doors, ushering in a new era, guaranteeing all Ontarians rights to privacy and access to government-held information. Justice Linden was followed by Tom Wright who oversaw the application of access and privacy laws to municipal institutions. In 1997, Ann Cavoukian was appointed Commissioner and would go on to serve for three terms. Dr. Cavoukian not only navigated the IPC through the fundamental shifts that the information technology revolution brought to the access and privacy worlds, she also elevated the IPC to an agency recognized for leadership in promoting privacy and freedom of information. I welcome the challenge and commit to building on this extraordinary legacy.

The widespread use of information technology tools that we have seen over a number of years will continue to present privacy challenges. The last decade alone has seen exponential advancements in mobile and other technologies which facilitate the collection, use and disclosure of vast amounts of personal information.

In 2014, we commemorated the 10th anniversary of the *Personal Health Information Protection Act*, which gives all Ontarians legislated protections when it comes to their personal health information. Today the legislation serves as a benchmark for other health privacy statutes across Canada.

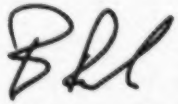
The widespread use of information technology tools that we have seen over a number of years will continue to present privacy challenges. The last decade alone has seen exponential advancements in mobile and other technologies which facilitate the collection, use and disclosure of vast amounts of personal information. Many of these technologies promise increased accountability and transparency – like police body-worn cameras. Others promise enhanced safety and security – like the outward facing cameras deployed by public transit vehicles and CCTV surveillance systems. It is imperative that these technologies are implemented in a manner that is consistent with the law and protects privacy.

Commissioner's Message

Government institutions are under pressure to respond more effectively to individuals in need of services, with limited resources. Consequently, institutions are streamlining service delivery models and looking for other opportunities to improve efficiency. These initiatives present unique privacy concerns when they involve the sharing of personal information across agencies. We are committed to working in a spirit of collaboration with stakeholders to ensure that accountability, public safety and security, and the effective use of government resources, are achieved in a privacy-protective manner.

No technology has transformed the way we live and work today more than the Internet. It enables the rapid dissemination of massive amounts of information within a short period of time for use in previously unimaginable ways. While presenting privacy challenges, technology also holds promise for promoting open and accountable government. In its report, *Open by Default: A New Way Forward for Ontario*, the province's Open Government Engagement Team recognizeu the benefits of making government held information readily available to the public. The team recommended that the government: establish Ontario as Canada's leader in public engagement; publish key documents online and in an open format; launch a "one-stop" Open Government platform and app that consolidates information; and develop partnerships to promote citizen engagement through the use of data for economic, social and policy development. I am pleased that the Premier has endorsed the findings of the Open Government Engagement Team and I urge the province to quickly take action and implement its recommendations. Open and transparent government is crucial to the democratic principles that we, as Ontarians, value.

The IPC has spent over two decades assisting municipal and provincial government organizations in addressing access and privacy issues. I look forward to reaching out and engaging with stakeholders and citizens from every corner of Ontario as we continue that work. Over the coming year, we will make significant efforts to strengthen our existing relationships and forge new ones through interaction, participation and cooperation. I believe we can best serve the interests of our province by working together in facing the challenges and seizing the opportunities that lie ahead.



Brian Beamish
Commissioner

We are committed to working in a spirit of collaboration with stakeholders to ensure that accountability, public safety and security, and the effective use of government resources, are achieved in a privacy-protective manner.

Access to Information

One of the fundamental purposes of the *Freedom of Information and Protection of Privacy Act (FIPPA)* and its municipal counterpart *(MFIPPA)* is to provide a right of access to government information, in accordance with the principle that it should be available to the public. This was reflected in the statement made by former Attorney General Ian Scott when he introduced *FIPPA* in the Legislature that, "we do not now, and never will, accept the proposition that the business of the public is none of the public's business." In recognition of this important principle, over more than two decades, we have advocated for a culture of openness in government through the creation of programs fostering greater disclosure. While we have seen some encouraging developments in the last few years, there is much more work to be done to ensure that institutions operate in an open and transparent way.

Open Government

The evolution of the Internet has created the opportunity to make a myriad of government information available in readily accessible formats for use in previously unimaginable ways. It has set new expectations for engagement on the part of the public for Open Government, empowering a more participatory democracy. Academics, researchers and business are also calling for the government to do a better job in treating its information as a public asset.

The possibilities and benefits of Open Government are endless. A truly open government brings more transparency and accountability; an informed public that is better able to participate in the decision-making process through meaningful, consultative engagement; and economic spinoffs from research and innovation to the benefit of business, government and the public.

In March, the Open Government Engagement Team, which was appointed by the Premier in 2013, released its report, *Open by Default: A New Way Forward for Ontario*, in which it made a number of recommendations aimed at promoting openness, including that the government:

- Reform *FIPPA* and *MFIPPA* by basing them on the principles of Open by Default and requiring the proactive publication of certain types of information.
- Launch a "one-stop" Open Government platform and app that consolidates information for all of its public engagement initiatives.
- Require ministries to pay for all costs associated with access to information requests when a ministry fails to meet the timelines for responding to a request, and the information is held on IT systems purchased in or after 2017.

The evolution of the Internet has created the opportunity to make a myriad of government information available in readily accessible formats for use in previously unimaginable ways.

We commend the team for this important work and fully support its recommendations. While the government has taken some important first steps to implementing the recommendations, including the publication of the Premier's ministers' mandate letters following the general election, there is still much work for the government to do. In her mandate letter, the Deputy Premier, who is also President of the Treasury Board, was given responsibility for leading the government's ongoing response to the engagement team's recommendations. We are prepared to lend our expertise to this effort.

Significant Access Decisions

The IPC issued a number of important orders this year which gave direction on how access to information legislation should be applied.

School Transportation

In 2006, the Ministry of Education initiated a series of reforms to the provision of student transportation by school boards. One of the central reforms allowed school boards to join together to establish a local "transportation consortium" to streamline costs, eliminate duplicate administrative duties and economize on transportation. These consortiums are financed by the participating school boards from their share of transportation funding from the ministry. A number of requests were made to different school boards seeking access to student transportation procurement records from some of these consortiums. Each board denied access to the records on the basis that the consortiums, as independent entities, had control of the records, and the records were therefore not in the custody or control of the boards. The IPC decided that each of these consortiums was part of the school boards to which the requests were made, and not distinct entities, regardless of whether they were incorporated. Further, given that the school boards direct and own the consortiums, the boards had control over the records. As a result, in six orders (MO-3141, MO-3142, MO-3143, MO-3144, MO-3145, MO-3146), we directed the relevant school boards to issue new access decisions.

Police Misconduct

In Order PO-3424-I, we decided that the Ministry of Community Safety and Correctional Services could not treat records relating to a police misconduct proceeding as excluded from *FIPPA*. The ministry had claimed that all of the requested records related to an "ongoing prosecution" and therefore were covered by the exclusion in section 65(5.2). In this case, an investigation by the Ontario Provincial Police led to a charge of disgraceful conduct against a Royal Canadian Mounted Police member under the RCMP's Code of Conduct. Our adjudicator decided that offences under the Code of Conduct do not lead to penal consequences, such as imprisonment or a fine. As a result, the exclusion did not apply because there was no "prosecution" within the meaning of *FIPPA*. We rejected the ministry's claim but allowed the ministry to provide submissions on whether other exemptions apply.

While the government has taken some important first steps to implementing the recommendations, including the publication of the Premier's ministers' mandate letters following the general election, there is still much work for the government to do.

Academic Freedom

Section 65(8.1) of *FIPPA* allows for certain research-related records to be excluded from the right of access, recognizing the importance of academic freedom and competitiveness of research conducted by universities and hospitals. This exclusion was at issue in Order PO-3365, relating to a request to the Ministry of Finance for records created by an expert panel convened to advise the Financial Services Commission of Ontario (FSCO) on potential reforms to Ontario's automobile insurance regulations. The records at issue included panel members' communications, meeting notes and exchanges with FSCO staff, created during the production of two published reports. In order for the exclusion to apply, two components are necessary: the records have to fit the definition of research, and the work must be conducted by a person associated with an educational institution or hospital. Although we accepted that the work was "research," it did not meet the second criterion. Although the chair of the panel conducting and directing the research was an employee of a research hospital and associated with a university, we found that the work of the panel members was not done in pursuit of their academic or clinical research goals, under the auspices of those institutions, but for the benefit of the government. As a result, we decided that the records were not excluded from *FIPPA*. Many of the records were exempt, however, as "advice or recommendations."

Section 65(8.1) of *FIPPA* allows for certain research-related records to be excluded from the right of access, recognizing the importance of academic freedom and competitiveness of research conducted by universities and hospitals.

Judicial Reviews

The Supreme Court of Canada (SCC) issued two important rulings on IPC decisions. In a strong endorsement of the IPC's expertise, the court stated in its reasons for judgment in the first case below that, "as an expert in privacy rights, as well as in access to information requests, the Commissioner's decisions deserve deference, short of an unreasonable conclusion falling outside the range of possible and acceptable outcomes."

Sex Offender Registry

In Order PO-2811, we directed the Ministry of Community Safety and Correctional Services to disclose to a media requester an aggregate statistical list showing the number of registered sex offenders residing within geographic areas encompassed by the first three characters of each postal code. These numbers were compiled from the Ontario Sex Offender Registry, which requires convicted sex offenders to register with local police services and to keep information about their residence updated. We rejected the ministry's argument that disclosure of the partial postal codes would facilitate the identification of sex offenders or reveal their addresses. We also rejected the position that offenders would fail to comply with registration requirements out of fear of harassment.

After lower court rulings on this issue, an appeal was heard by the SCC. The ministry claimed that the adjudicator applied too onerous a standard of proof for showing a potential for future harm to public safety or the ability of police to control crime. The SCC rejected the ministry's arguments and dismissed its appeal, resulting in the release of the record and media publication of the information.

Advice and Recommendations

The SCC discussed the "advice or recommendations" exemption relating to a request to the Ministry of Finance for records which considered the "pros and cons" of proposed changes to corporate tax legislation. The ministry cited the section 13 exemption that allows an institution to refuse to disclose a record if it reveals the "advice and recommendations" of a public servant, public employee, or a consultant retained by the institution. The adjudicator decided that, in order to be covered by the exemption, the information must suggest a course of action which will be accepted or rejected by the person being advised. These records did not suggest a particular course of action and did not contain a recommended course of action. There was also no evidence from the records that the information was actually communicated to the decision-maker. We therefore ordered the records to be disclosed, in Order PO-2872.

The Ministry of Finance appealed this ruling all the way to the SCC and was ultimately successful in overturning the IPC's approach. In its ruling, the SCC determined that records that include various options for a decision-maker to consider, not just information revealing a single suggested course of action, also contain "advice." The court described the language in section 13 as broad, encompassing various records relating to the deliberative process of government decision-making, including options and their "pros and cons." It also decided that it was not necessary that the advice actually be communicated to the decision-maker.

Recommendation

For many years we have encouraged the government to embrace the Open Data and Open Government movements. Without access to information held by institutions, citizens cannot participate meaningfully in the democratic process or hold their elected officials accountable. Government-generated data sets and records also have a growing value and have the potential to drive innovation in an information economy. We applaud the government for establishing the Open Government Engagement Team and encourage it to proceed immediately with implementing its recommendations.

Protection of Privacy

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and its municipal counterpart *(MFIPPA)* establish rules for how and when institutions may collect, use and disclose personal information. To ensure compliance with these rules, we have the authority to comment on the implications of proposed legislative schemes, or government programs and information practices. In fulfilling that role, we provide guidance on new technologies or practices and procedures that have the potential to impact privacy. In 2014, we undertook significant work in privacy protection, including the four examples highlighted below.

Situation Tables

Across the province, a number of important pilot projects have been initiated to facilitate greater collaboration among diverse agencies, including law enforcement, health-care, housing and income support service providers. The goal of these projects is to provide interdisciplinary solutions to better assist individuals who are in need of urgent assistance. These projects, referred to as situation tables, involve the sharing of personal information among distinct organizations. The goals of these initiatives are laudable but they do raise a variety of privacy concerns. It is essential that situation tables comply with existing legislation and that they operate in a privacy-protective manner.

While we believe it is possible to develop a collaborative model for information sharing in urgent circumstances that respects privacy and complies with the law, there is work to be done in this area.

Our primary concern is ensuring appropriate governance for these models. Participants in the pilot projects need training and guidance on responsible information-sharing practices including an understanding of de-identification, data minimization and the legal authority to collect, use and disclose personal information. In addition, practices and protocols should be developed to ensure that the information-sharing activities are documented as part of a transparent and accountable process.

We encourage the Ministry of Community Safety and Correctional Services to develop tools and guidelines to assist situation table participants, and we have expressed our willingness to work with the ministry to address the privacy issues that may arise.

Police Body-Worn Cameras

Body-worn cameras are compact audio and video recording devices that can be worn by police to record interactions with members of the public. Proponents of the cameras believe that this technology will improve transparency and accountability for police actions, and there appears to be significant public support for the use of these devices. In fact, the use of this technology is growing, with a number of police services running pilot projects.

The use of body-worn cameras raises significant privacy issues since the technology involves the collection and retention of a wide array of personal information. These cameras may capture information about bystanders, images within private places (residences), and extremely sensitive details involving victims of crime. Law enforcement agencies must develop standards relating to notice, use and disclosure. Individuals' right to access their own information and the security of the

footage, including appropriate disclosure, retention and secure destruction, are also considerations. It must also be recognized that when other technologies, such as facial recognition, are combined with the use of body-worn cameras, different privacy issues arise. These challenges do not represent barriers to the implementation of these devices, if properly addressed.

We have had preliminary consultations with several Ontario police services on body-worn cameras, and we welcome any other service considering the use of this technology to contact us for assistance. To offer guidance, we, along with our federal, provincial and territorial colleagues across Canada, released guidelines in 2015, which identified the key privacy considerations law enforcement agencies should take into account before operationalizing body-worn cameras. In addition, we would be pleased to assist the provincial government if it decides to develop its own guidelines on the use of this technology.

Across the province, a number of important pilot projects have been initiated to facilitate greater collaboration among diverse agencies, including law enforcement, health care, housing and income support service providers.

Crossing the Line

In late 2013, the IPC investigated complaints from several Ontarians who were denied entry into the United States because of their mental health history. We discovered that some police services were sharing sensitive information about attempted suicides via the Canadian Police Information Centre (CPIC), a national law enforcement and public safety database maintained by the Royal Canadian Mounted Police (RCMP). We then found out that United States border officials have access to CPIC and are relying on this information to deny individuals entry into the country.

During our investigation, we interviewed a number of individuals who had been stopped at the border, reviewed the practices of several Ontario police services, and consulted with mental health organizations. We learned that there were significant variations in the way police services were dealing with this sensitive information, and concluded that the uploading of information about all attempted suicides does not comply with *FIPPA* and *MFIPPA*.

In our report, *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC*, we outlined a four-part mental health disclosure test that police must use to assess whether or not attempted suicide information should be added to CPIC. To justify disclosure, one of the following four circumstances must exist: threat of serious violence or harm to others; intentional provocation of a lethal response by the police; history of serious violence or harm to others; or suicide attempt while in police custody.

Though the majority of police services we consulted with agreed to implement our recommendations, the Toronto Police Service refused to change its practice of sharing information via CPIC about all attempted suicides, regardless of the circumstances. As a result, the IPC filed an application with the Ontario Superior Court requesting an order that the Toronto Police Service stop this practice. We anticipate that the case will be heard in 2015.

Police Record Checks

For nearly a decade, the IPC has been closely involved in efforts to modernize the way law enforcement agencies perform police record checks (PRCs) that employers and other third parties are increasingly requiring from job applicants and volunteers. PRC practices have led to the disclosure of information about far more than criminal convictions. Some police routinely disclose non-conviction information (e.g. acquittals and withdrawn charges) and non-criminal information (e.g. mental health incidents). These disclosures can unfairly affect an individual's employment and volunteer opportunities.

In response to numerous complaints and inquiries, we have issued investigation reports, intervened before the courts, and participated in public consultations with the Ontario Human Rights Commission, the Ontario Association of Chiefs of Police (OACP), and civil society groups. We have consistently recommended that non-conviction and non-criminal information should be disclosed by police in a PRC only in exceptional circumstances, based on objective public safety-related criteria.

Consultations: Legislation, Programs and Information Practices

The following list provides a sampling of the advice and consultation work done by the IPC during 2014:

Provincial Consultations:

Adoption Council of Ontario
- Online Child-Specific Recruitment of Adoptive Parents

Financial Services Commission of Ontario
- Changes to Consent Language in Ontario Auto Insurance Forms

Ministry of Citizenship, Immigration and International Trade
- Bill 49 – *Ontario Immigration Act, 2014*

Ministry of Education
- Bill 10 – *Child Care Modernization Act, 2014*
- Ontario Registry of Unlicensed Child Care Violations

Ministry of Finance
- Bill 56 – *Ontario Retirement Pension Plan Act (Requirement to Establish), 2014*
- Ministry Offices' Video Surveillance Policy

Ministry of the Attorney General
- Administrative Child Support Online Calculation Service

Ministry of Training, Colleges and Universities
- Bill 10 – Schedule 4 Amendments to the *Education Act*
- Bill 10 – Schedule 5 Amendments to the *Ministry of Training, Colleges and Universities Act*

Ontario Association of Chiefs of Police
- Police Record Checks
- Victim Services Groups

OPP/Integrated Security Unit – Integrated Community Liaison Team
- Pan Am/Parapan Am Games Consultation

Municipal Consultations:

Crime Prevention Ottawa
- Multi-Stakeholder Approach to Problem Addresses

Region of Peel
- Social Services Delivery Model
- Information Sharing Within the Human Services Department

Stratford Police Service
- Automated Licence Plate Recognition Pilot

Toronto Police Service
- Body-Worn Camera Pilot
- Police and Community Engagement Review
- Public Space CCTV Procedure
- Facial Recognition Technology Pilot

Toronto Transit Commission
- CCTV Surveillance

Our PRC work has included participating in the development of the OACP's Law Enforcement and Records (Managers) Network (LEARN)'s *Guidelines for Police Record Checks*. We applaud the OACP for its leadership in this area; however, police services have been left to choose whether or not to adopt these non-binding guidelines. Since PRCs have become far more routine, we believe that a binding provincial standard is required to ensure that these disclosures are appropriately constrained and take place on the basis of the careful exercise of discretion.

The government has recognized the need for a uniform approach for PRCs, and in late 2014 stated that it will be tabling legislation to address this. We will continue to work with the Ministry of Community Safety and Correctional Services as it moves towards the development of a solution to this important issue.

Recommendation

Ontarians would greatly benefit from a legislated standard that articulates what information may be disclosed in a PRC. A uniform province-wide approach must also include improvements to transparency and accountability, as well as a right of appeal. We will continue to press for the early enactment of an appropriate provincial standard. As media reports have reminded us, poorly designed PRC programs can have damaging and unfair impacts on individuals.

PHIPA 10th Anniversary

The *Personal Health Information Protection Act (PHIPA)* establishes rules governing the collection, use and disclosure of personal health information (PHI) within the health sector. This statute was 24 years in the making, beginning with the Krever Commission in 1980, which examined allegations of improper police access to patient records. Ten years after being enacted, *PHIPA* is still considered the gold standard among health privacy statutes, influencing other privacy legislation across Canada.

Unauthorized Access

We continue to see instances where health-care workers have accessed the PHI of individuals to whom they are not providing care, and for purposes that are not authorized.

For example, within a 12-month period, the Rouge Valley Health System (the hospital) reported two separate privacy breaches to us. Both involved allegations that hospital employees had accessed the electronic medical records of new mothers, for the purpose of marketing Registered Education Savings Plans. In reviewing the matter, we learned that the hospital was unable to audit how information was being accessed, due to technical limitations. The hospital's failure to implement adequate audit measures meant that it could not comply with its own policies or *PHIPA*. We also determined that the hospital had insufficient privacy policies, which are critical in protecting PHI.

As a result of our review, we issued Order HO-013, requiring the hospital to implement measures to ensure that its auditing capabilities were fully functional and that it was able to check all instances where PHI was accessed. We also ordered the hospital to work with its software provider to develop a solution that will prevent open-ended searches. Additionally, we ordered the hospital to revise its privacy policies and implement a training program for all staff.

Despite this order, unauthorized access continues to be an issue – its impact is real and can have serious consequences for both patients and the health sector as a whole.

Unauthorized access can result in discrimination, stigmatization and psychological harm to patients. It may also result in patients avoiding treatment or withholding or providing false information to their health-care provider, as well as a loss of trust or confidence in the health system. In addition, unauthorized access can result in disciplinary action, damage to reputation, investigations and orders, costly legal actions and prosecutions. While health-care workers have been dismissed for violating patient privacy, this may not be enough of a deterrent. Under *PHIPA*, unauthorized access to PHI can result in prosecutions with fines of up to $50,000 for individuals and $250,000 for organizations. Given the prevalence of unauthorized access, it may be necessary to increase the number of prosecutions

We continue to see instances where health-care workers have accessed the PHI of individuals to whom they are not providing care, and for purposes that are not authorized.

to send a strong message that unauthorized access will not be tolerated. We have engaged in discussions with the Ministry of Health and Long-Term Care and the Attorney General's office to facilitate the referral of cases of unauthorized access for prosecution.

Protection of privacy should be integral to the delivery of health care and embedded into the culture of health-care organizations. Developing and implementing a comprehensive approach to the protection of privacy and the confidentiality of PHI is essential. Health-care organizations must put in place strong policies and training, which will go a long way toward preventing unauthorized access.

We have engaged in discussions with the Ministry of Health and Long-Term Care and the Attorney General's office to facilitate the referral of cases of unauthorized access for prosecution.

Prescribed Entities and Registries

PHIPA permits health information custodians (HICs) to disclose personal health information, without consent, to prescribed entities for the purpose of analysis or compiling statistical information needed to plan and manage the health system. Similarly, HICs are permitted to disclose PHI without consent, to prescribed persons that compile or maintain registries of personal health information for the purposes of facilitating or improving the provision of health care.

Every three years, we review the information practices and procedures of prescribed entities and persons. In 2014, we reviewed:

Prescribed Entities

- Cancer Care Ontario
- Canadian Institute for Health Information
- Institute for Clinical Evaluative Sciences
- Pediatric Oncology Group of Ontario.

Prescribed Registries

- Cardiac Care Network of Ontario in respect of its registry of cardiac services
- INSCYTE Corporation in respect of CytoBase
- Cancer Care Ontario in respect of the Ontario Cancer Screening Registry
- Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network
- Ontario Cancer Research Institute in respect of the Ontario Tumour Bank
- Hamilton Health Sciences Centre in respect of the Critical Care Information System.

We found that all of the above prescribed entities and persons continue to meet the requirements of *PHIPA*. Reports, affidavits and approval letters for each of these reviews are available on our website.

ConnectingPrivacy

Shared electronic health records (EHRs) give multiple health-care providers the ability to contribute information to, and collect information from, a single system, where custody and control of the information is shared among the providers. It is imperative that providers participating in such systems establish a governance framework that sets out how the duties and obligations in *PHIPA* will be satisfied in a shared EHR environment, and that ensures individuals are able to exercise their rights seamlessly. It must include harmonized privacy policies addressing, at a minimum, consent management, auditing, access and correction, complaints, and privacy breach management. To facilitate compliance, initial and ongoing training must be mandatory. This will help to instill trust and confidence among patients and providers that privacy of PHI in these systems is being protected.

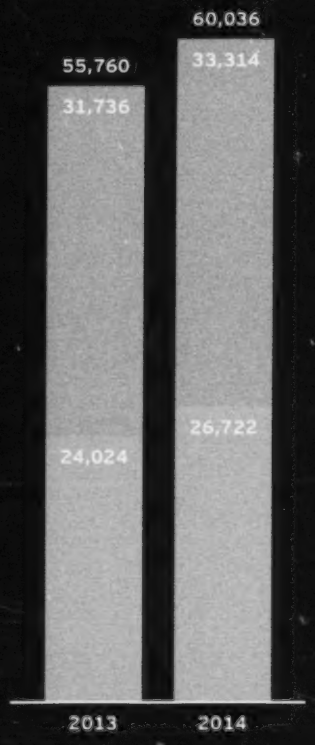
We are participating in the ConnectingPrivacy committee, which was established by eHealth Ontario, to develop a harmonized privacy governance framework for shared electronic health records. Our goal is to ensure a consistent approach to privacy protection across shared regional EHR systems.

Recommendation

EHRs have the potential to improve treatment, enhance safety, and facilitate the coordination of services, resulting in a more efficient and effective health-care system. Over the coming years, Ontario's health-care system will need to adapt to rapid changes in technology, including EHRs. Consequently, there is a growing need for a legislative framework to address PHI in an increasingly digital and interconnected world.

While *PHIPA* has served Ontario admirably over the last decade, it does not adequately address the rights of individuals and the duties of HICs in an EHR environment. The IPC recommends that the government re-introduce the *Electronic Personal Health Information Protection Act.* This legislation will amend *PHIPA* to clarify how the privacy of patients and the confidentiality of their PHI will continue to be protected as the health-care sector transitions to electronic systems.

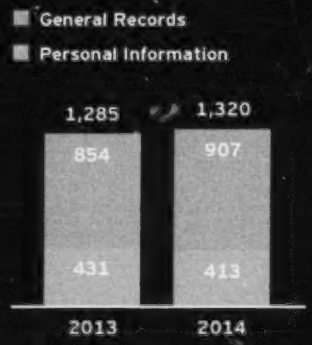
Overall Requests



Total Requests	↑ 8%
General Records	↑ 5%
Personal Information	↑ 11%

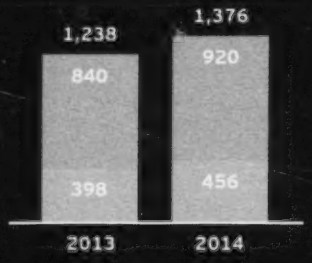
Overall Appeals

Appeals Opened



Total Appeals Opened ↑ 3%

Appeals Closed



Total Appeals Closed ↑ 11%

2014 At a Glance

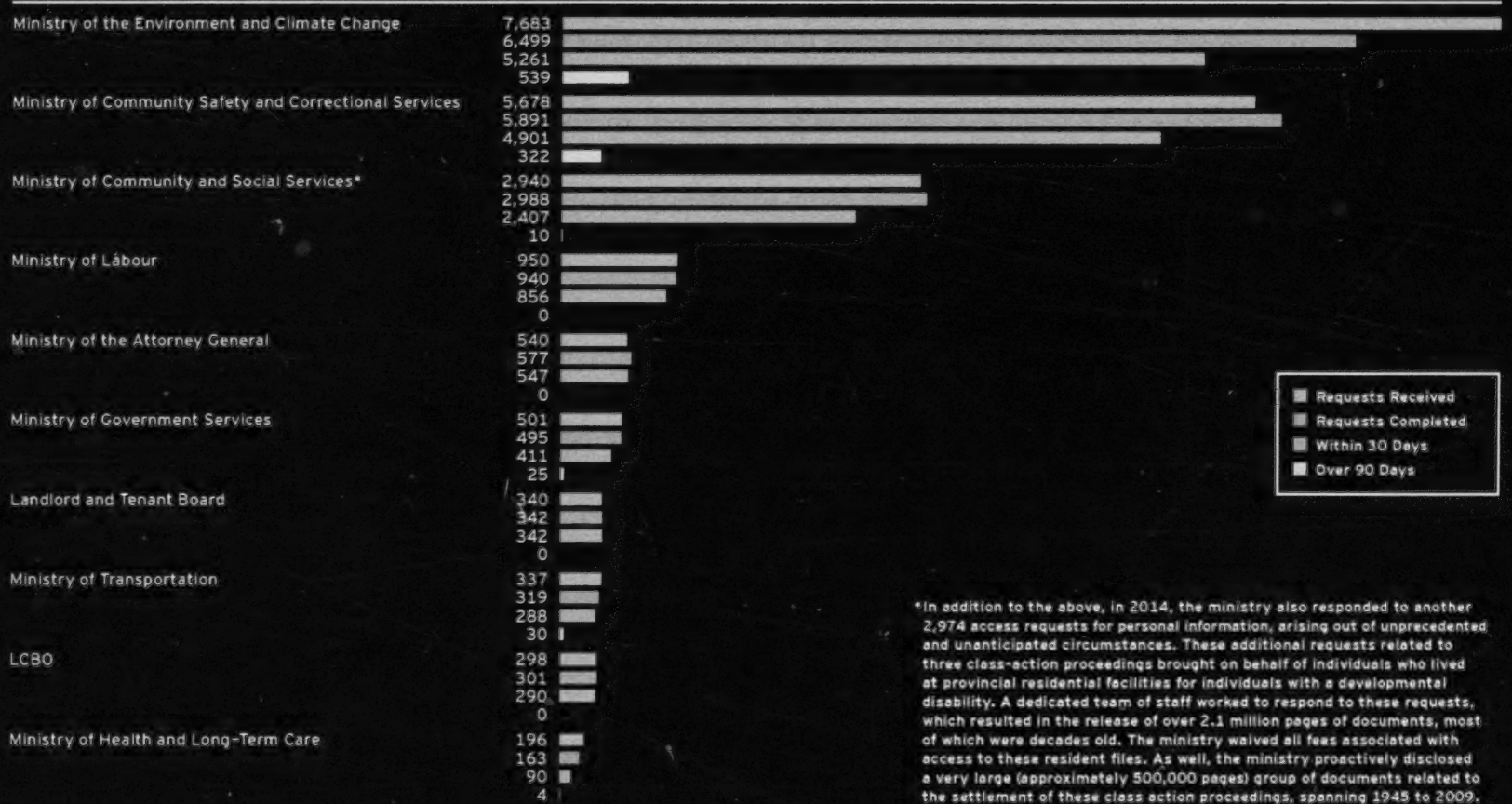
Provincial Statistics

	Personal Information	General Records	Totals
Requests	2014 8,241 2013 7,029 ↑ 17%	2014 16,666 2013 14,402 ↑ 16%	Total Requests 2014 24,907 2013 21,431 ↑ 16%
Appeals Opened	2014 194 2013 186 ↑ 4%	2014 501 2013 421 ↑ 19%	
Appeals Closed	2014 201 2013 143 ↑ 41%	2014 497 2013 454 ↑ 9%	Privacy Complaints Opened 2014 123 2013 120 ↑ 2%
Average Cost	2014 $4.47 2013 $6.04 ↓ 26%	2014 $41.48 2013 $40.57 ↑ 2%	Privacy Complaints Closed 2014 143 2013 118 ↑ 21%

Municipal Statistics

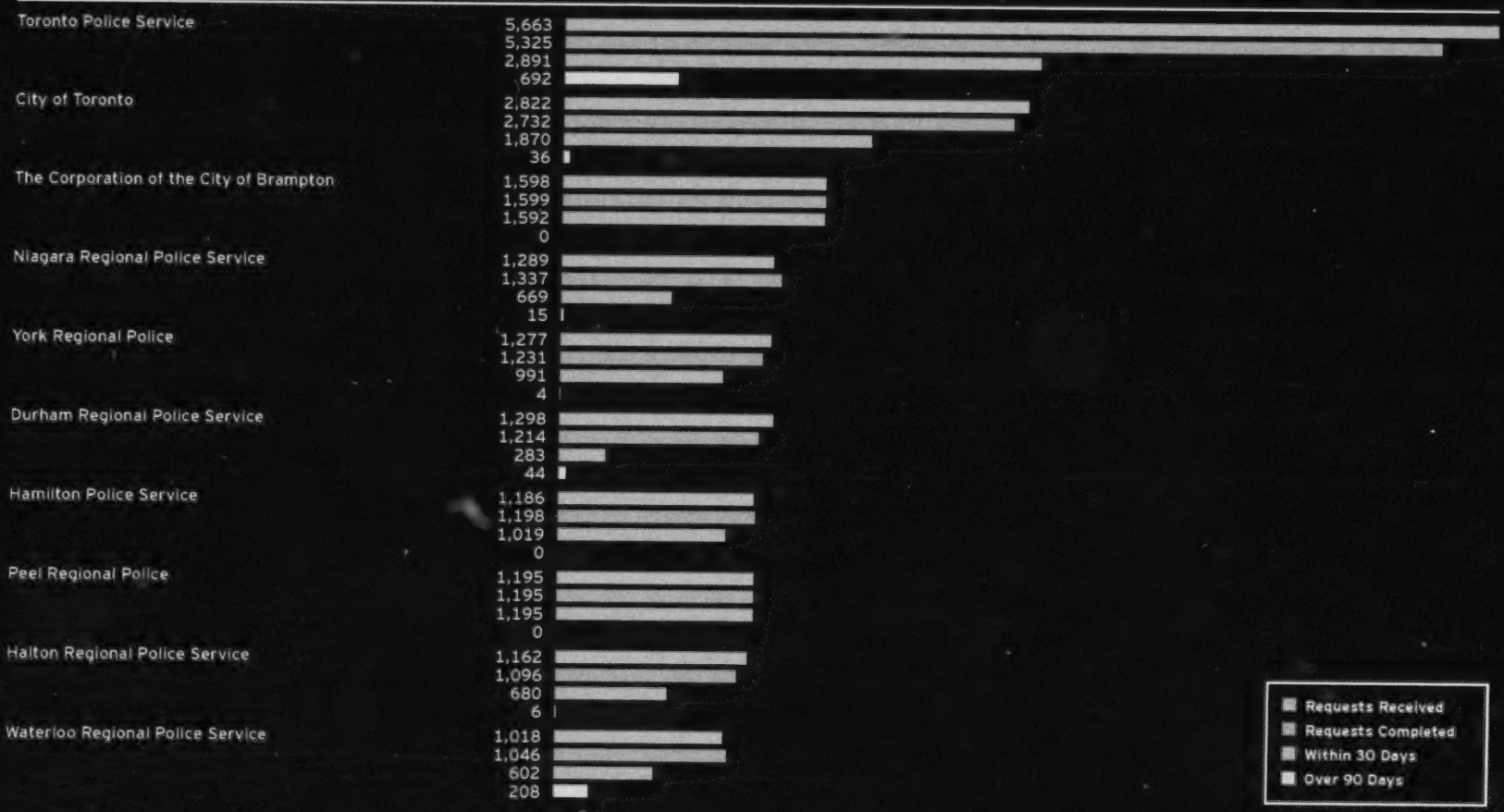
	Personal Information	General Records	Totals
Requests	2014 18,481 2013 16,995 ↑ 9%	2014 16,648 2013 17,334 ↓ 4%	Total Requests 2014 35,129 2013 34,329 ↑ 2%
Appeals Opened	2014 219 2013 245 ↓ 11%	2014 406 2013 433 ↓ 6%	
Appeals Closed	2014 255 2013 255 ■ 0%	2014 423 2013 386 ↑ 10%	Privacy Complaints Opened 2014 157 2013 136 ↑ 15%
Average Cost	2014 $8.86 2013 $8.24 ↑ 8%	2014 $26.03 2013 $28.09 ↓ 7%	Privacy Complaints Closed 2014 133 2013 141 ↓ 6%

Top 10 Provincial Institutions



*In addition to the above, in 2014, the ministry also responded to another 2,974 access requests for personal information, arising out of unprecedented and unanticipated circumstances. These additional requests related to three class-action proceedings brought on behalf of individuals who lived at provincial residential facilities for individuals with a developmental disability. A dedicated team of staff worked to respond to these requests, which resulted in the release of over 2.1 million pages of documents, most of which were decades old. The ministry waived all fees associated with access to these resident files. As well, the ministry proactively disclosed a very large (approximately 500,000 pages) group of documents related to the settlement of these class action proceedings, spanning 1945 to 2009.

Top 10 Municipal Institutions



FOI Requests and Appeals

FOI Requests Completed by Source

Individual/Public	27,483
Individual by Agent	10,857
Business	13,635
Academic/Researcher	346
Association/Group	729
Media	1,045
Government (all levels)	1,200
Other	601
Total Requests	**55,896**

Outcome of FOI Requests

All Information Disclosed	15,098
Information Disclosed in Part	25,207
No Information Disclosed	4,889
No Responsive Records Exist	7,060
Request Withdrawn, Abandoned or Non-Jurisdictional	3,642
Total Requests	**55,896**

Issues in Appeals Opened

Exemptions only	511
Third Party	144
Deemed Refusal	136
Reasonable Search	113
Exemptions with Other Issues	108
Act Does Not Apply	97
Other	74
Interim Decision	46
Time Extension	23
Frivolous or Vexatious	17
Fee and Fee Waiver	12
Correction	11
Custody or Control	11
Fee	7
Fee Waiver	6
Failure to Disclose	3
Transfer	1
Forward	0
Inadequate Decision	0
Total	**1,320**

Outcome of Appeals by Stage Closed

Mediated in Full	737
Order Issued	310
Withdrawn	151
Screened out	93
Abandoned	51
Dismissed without Inquiry/ Review/Order	34
Total	**1,376**

Appeals Closed by Order by Order Outcome

Head's decision upheld	144
Head's decision partially upheld	116
Head's decision not upheld	46
Other	4
Total	310

Health Privacy

PHIPA At a Glance

Requests Completed

2014	85,156
2013	109,529

↓ 22%

Request Average Cost

2014	$17.20
2013	$16.06

↑ 7%

Complaints Opened

2014	439
2013	407

↑ 8%

Complaints Closed

2014	399
2013	381

↑ 5%

Types of *PHIPA* Complaints Opened

Access and Correction	111
Collection, Use and Disclosure	120
Self-reported breach	172
IPC-initiated	36
Total	**439**

PHIPA Complaints by Custodian Type

Public Hospital	161
Clinic	71
Doctor	51
Other health care professional	26
Community Care Access Centre	22
Community or Mental health centre, program or service	22
Pharmacy	14
Independent Health Facility	12
Other	9
Ministry of Health	8
Laboratory	5
Dentist	4
Institution – *Mental Hospitals Act*	4
Other prescribed person	4
Home for special care	3
Home or joint home (aged or rest)	3
Long-term care facility	3
Agent	2
Health Data Institute	2
Optometrist	2
Psychologist	2
Chiropractor	1
Dental Hygienist	1
Masseur	1
Nursing Home	1
Occupational Therapist	1
Physiotherapist	1
Private Hospital	1
Psychiatric Facility	1
Social Worker	1
Total	**439**

Privacy Complaints

Issues In Privacy Complaints

Disclosure	156
Security	16
Collection	13
Use	7
General privacy issue	6
Personal information	3
Disposal	1
Consent	1
Access	1
Total	**204**

Outcome of Issues in Privacy Complaints

Resolved – Finding not necessary	177
Complied in Full	16
Act does not apply	8
Not Complied	3
Total	**204**

Judicial Reviews

New Judicial Review Applications by Applicant Type

Institution	1
Requester/Complainant	7
Affected Party	3
IPC intervened in other application or appeal	2
IPC-initiated application	1
Total	**14**

Outstanding Judicial Review Applications by Applicant Type

Institution	5
Requester/Complainant	6
Affected Party	4
IPC intervened in other application or appeal	1
IPC-initiated application	1
Total	17

Judicial Reviews Closed and/or Heard in 2014

Abandoned or settled or dismissed for delay – IPC Order stands	11
IPC Order upheld (and/or leave to appeal dismissed)	3
IPC Order not upheld (and/or IPC's leave to appeal dismissed) and matter remitted back to IPC	3
IPC Order upheld on SCC appeal	1
IPC Order not upheld on SCC appeal	2
IPC intervened in SCC or Federal Court appeal	2
Total	**22**

Financial Statement

	2014–2015 Estimates $	2013–2014 Estimates $	2013–2014 Actual $
Salaries and wages	10,444,100	10,211,500	9,146,774
Employee benefits	2,625,900	2,348,900	1,820,306
Transportation and Communications	337,500	337,500	255,082
Services	1,960,300	1,960,300	1,857,857
Supplies and Equipment	336,000	336,000	404,193
Total	15,703,800	15,194,200	13,484,212

Note: The IPC's fiscal year begins April 1 and ends March 31.

The full set of the financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario in accordance with the financial reporting provisions of the Legislative Assembly Act, which requires the statement be prepared on a modified cash basis rather than using public sector accounting standards.

2014 Appeals Fees Deposit

(Calendar year)	$
General Information	15,425
Personal Information	3,280
Total	18,705

How to Reach Us

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Toronto Area: 416-326-3333
Long Distance: 1-800-387-0073 (within Ontario)
TDD/TTY: 416-325-7539

www.ipc.on.ca
info@ipc.on.ca